PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-037590
(43)Date of publication of application : 07.02.2003

(51)Int.Cl. H04L 9/14
G06F 12/14

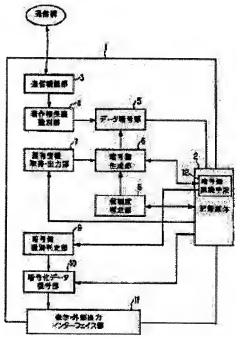
(21)Application number : 2001-380390
(22)Date of filing : 13.12.2001

(71)Applicant : SHARP CORP
(72)Inventor : EZURE KATSUYOSHI

(30)Priority
Priority number : 2001149824 Priority date : 18.05.2001 Priority country : JP

(54) INFORMATION PROCESSOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information processor with an encryption device, which can improve protection of the copyright to the received data and can deal with the life of a recording medium suitably.
SOLUTION: This processor is provided with a copyright protection identification part 4 to identify whether the received data is the data protected by the copyright or not and a reliability decision part 8 to decide the reliability of a recording medium 2. A encryption key is formed in the encryption key formation part 6 based on the prescribed information of the recording medium 2 in the case the reliability of the recording medium 2 is high in the reliability decision part 8 when the data identified that it is protected by the copyright in the copyright protection identification part 4 is enciphered. On the other hand, when it is determined that the reliability of the recording medium 2 is low, the encryption key is formed based on the prescribed information of the information processor 1.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－37590
（P2003－37590A）
(43)公開日　平成15年2月7日(2003.2.7)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/14		Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０		３２０Ｆ	５Ｊ１０４
		Ｈ０４Ｌ　9/00	６４１	

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

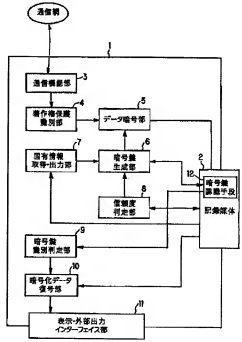
(21)出願番号　特願2001－380390(P2001－380390)
(22)出願日　平成13年12月13日(2001.12.13)
(31)優先権主張番号　特願2001－149824(P2001－149824)
(32)優先日　平成13年５月18日(2001.5.18)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　江迫　克佳
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100112335
弁理士　藤本　英介

Ｆターム(参考)　5B017 AA06 BA07
5J104 AA01 AA35 AA37 NA02 PA14

(54)【発明の名称】　情報処理装置

(57)【要約】
【課題】　受信したデータに対して、その著作権の保護を強化することが可能で、かつ記録媒体の寿命に適切に対応することが可能な暗号化装置を備えた情報処理装置を提供する。
【解決手段】　受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別部４と、記録媒体２の信頼度を判定するための信頼度判定部８とを備える。著作権保護識別部４において著作権により保護されていると識別されたデータに対して暗号化を行う際に、暗号鍵生成部６では、信頼度判定部８において記録媒体２の信頼度が高いと判定されると、記録媒体２の固有情報に基づいて暗号鍵を生成する。一方、記録媒体２の信頼度が低いと判定されると、当該情報処理装置１の固有情報に基づいて暗号鍵を生成する。



【特許請求の範囲】

【請求項１】　データを受信するための受信手段と、該受信手段により受信した受信データを暗号化するための暗号化手段と、該暗号化手段により暗号化した受信データを交換可能な記録媒体に記録するための記憶手段とを備え、前記記録媒体に記録された受信データを新規な記録媒体に複写可能な情報処理装置において、

前記受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別手段と、

前記記録媒体の信頼度を判定するための信頼度判定手段とを備え、

前記著作権保護識別手段において著作権により保護されていると識別されたデータに対して、前記暗号化手段により暗号化を行う際に、

前記信頼度判定手段において前記記録媒体の信頼度が高いと判定された場合には、前記記録媒体の固有情報に基づいて暗号鍵を生成して暗号化を行うとともに、

前記信頼度判定手段において前記記録媒体の信頼度が低いと判定された場合には、当該情報処理装置の固有情報に基づいて暗号鍵を生成して暗号化を行うことにより、著作権を保護することを特徴とする情報処理装置。

【請求項２】　前記記録媒体に記録されたデータに対して用いられている暗号鍵の種類を識別するための暗号鍵識別手段を備えたことを特徴とする請求項１記載の情報処理装置。

【請求項３】　前記記録媒体に対してデータを暗号化して記録する際に、当該記録媒体において前記暗号鍵の種類が混在しないようにすることを特徴とする請求項１記載の情報処理装置。

【請求項４】　データを受信するための受信手段と、該受信手段により受信した受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別手段と、前記受信データから著作権情報を検出して著作権管理情報を生成するための著作権情報管理手段と、前記受信データを暗号化するための暗号化手段と、該暗号化手段により暗号化した前記受信データを交換可能な記録媒体に記録するための記憶手段とを備え、前記記録媒体に記録された受信データを新規な記録媒体に複写可能な情報処理装置において、

当該情報処理装置の固有情報と、前記受信データの著作権情報と、前記著作権情報管理手段で生成した著作権管理情報とに基づいて暗号鍵を生成するための暗号鍵作成手段を備え、

前記受信データに対して、前記暗号鍵作成手段で作成した暗号鍵を用いて暗号化を行い暗号化済受信データを生成し、該暗号化済受信データを前記記録媒体に記録することを特徴とする情報処理装置。

【請求項５】　前記受信データの著作権情報が許可した範囲において、前記暗号化済受信データと、該暗号化済受信データを複合化するための暗号鍵を送出し、新規な記録媒体に複製可能としたことを特徴とする請求項４記載の情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、受信したデータに対して、その著作権の保護を強化することが可能な暗号化装置を備えた情報処理装置に関する。

【０００２】

【従来の技術】近年、データ通信が一般化するに伴い、通信機能を有した携帯情報端末装置が普及してきている。これらの携帯情報端末装置には、受信したデータを保存するための記録媒体を備えており、この記録媒体は、例えば、携帯情報端末装置に装着脱可能となった書き換え可能なメモリカードにより構成されている。また、これらの携帯情報端末装置では、受信したデータをメモリカード等の記録媒体に保管する際に暗号化する技術が採用されており、受信データの内容を他人が容易に読むことができないようになっている。

【０００３】例えば、特開平９－１４６４５７号公報には、情報記録媒体の固有の識別情報を任意の認証番号により暗号化して第１の情報を生成し、この第１の情報を情報記録媒体を取り扱うシステムの所定の情報により暗号化して第２の情報を生成し、この第２の情報の一部を選択して第３の情報を生成し、この第３の情報を情報記録媒体に対する情報の読み取りおよび書き込みを行うための装置の固有の情報により暗号化して情報記録媒体に記録される情報へアクセスするための暗号鍵を生成するようにした技術が開示されている。

【０００４】また、特開２０００－１８７９３５号公報には、通信手段により暗号化されたディジタルデータを受信するための通信手段を有するとともに、データの暗号化を行うための暗号化手段は、記録媒体の識別情報に基づいて生成した暗号鍵によりデータを暗号化するための第１の暗号化部と、記録媒体を取り扱う再生装置の識別情報に基づいて生成した暗号鍵によりデータを暗号化するための第２の暗号化部とを有し、記録媒体が再生装置から着脱可能であると判断した場合には、第１の暗号化部によりデータの暗号化を行なわせ、記録媒体が再生装置から着脱不可であると判断した場合には、第２の暗号化部によりデータの暗号化を行なわせるようにした技術が開示されている。

【０００５】また、特開平７－２８７６５５公報には、装置の固有情報を記録媒体に書き込んでおき、この記録媒体が装置に装着された時、装置の固有情報と、記録媒体上に記録済の固有情報を読み出して比較し、固有情報が一致しなかった場合はアクセスを禁止する技術が開示されている。この技術では、固有情報を記録媒体に記録する際に、固有情報を暗号化するようになっている。

【０００６】また、特開２０００－１１３５８６公報には、記録媒体の保持する固有情報によって暗号化された

鍵と、各情報に特有の識別情報と、前記鍵により暗号化された情報とに基づいて、暗号化された鍵を情報特有の識別情報により特定し、暗号化された情報を複合化して再生する技術が開示されている。

【０００７】

【発明が解決しようとする課題】上述した従来の技術においては、種々の暗号鍵生成方式により生成された暗号鍵を用いて、記録媒体に記録される情報の安全性を高めたり、記録媒体が着脱可能な場合に、暗号鍵の生成方式を制御する方法が採用されている。すなわち、データ秘匿の重要性が増すことにより、その安全性にかかわる暗号鍵の生成および制御はより高度になってゆく。さらに、データを記録するための記録媒体には物理的（電気的）な寿命があることから、データの複写を行い、バックアップしておくことが重要となってくる。

【０００８】しかしながら、上述した従来の技術では、着脱可能な記録媒体に対して、当該記録媒体の識別情報に基づいて暗号鍵を制御する方法が採用されている。このため、当該記録媒体のデータを新規な記録媒体に複写すると、元の記録媒体の固有情報と新規な記録媒体の固有情報とが異なることから、複写はできても再生ができなくなってしまうという問題があった。

【０００９】また、情報処理装置の固有情報を記録媒体に書き込む方式では、上述した問題を解決することができるものの、データの著作権を無視して複写がなされる可能性が生じるという問題があった。すなわち、データの暗号化に対しである程度の知識を有する者であれば、記録媒体に記録されている暗号化データを一旦復号化して再生し、次に保存する場合に、新規な記録媒体に対してデータを保存すれば、著作権を無視した複写を行うことができてしまう場合があった。

【００１０】また、記録媒体の固有情報に基づいて暗号鍵を生成する方法では、記録媒体自体の寿命や使用環境による寿命（エラーレートの増加）に対応して、記録媒体に記録されたデータを複写することができなかった。すなわち、従来の技術では、ユーザが記録媒体の寿命を知るための手段がないため、ユーザによっては、記録媒体のデータが永久に使用できると思いこんでしまうケースが多々見受けられた。

【００１１】また、装置の固有情報と、記録媒体上に記録済の固有情報とを読み出して比較し、固有情報が一致しなかった場合はアクセスを禁止する方法では、記録媒体に記録された情報自体は容易に読み出せるため、別の記録媒体に複製が可能であり、著作権の保護を図ることができなかった。さらに、装置が故障などにより使用不可能となった場合には、それまで記録された情報を他の装置で読み込もうとしても、記録媒体に書き込まれた装置の固有情報が異なるため、読み出しが不可能であった。

【００１２】また、記録媒体の保持する固有情報によって暗号化された鍵と、各情報に特有の識別情報と、前記鍵により暗号化された情報とに基づいて、暗号化された鍵を情報特有の識別情報により特定し、暗号化された情報を複合化して再生する方法では、各情報に特有の識別情報を利用すれば、各情報を無制限に複製できるので、著作権保持者が望む複製回数の制限が無効となり、結果として著作権保護を図ることができなかった。

【００１３】本発明は、上述した事情に鑑み提案されたもので、受信したデータに対して、その著作権の保護を強化することが可能で、かつ記録媒体の寿命に適切に対応することが可能な暗号化装置を備えた情報処理装置を提供することを目的とする。

【００１４】

【課題を解決するための手段】本発明に係る情報処理装置は、データを受信するための受信手段と、該受信手段により受信した受信データを暗号化するための暗号化手段と、該暗号化手段により暗号化した受信データを交換可能な記録媒体に記録するための記憶手段とを備え、前記記録媒体に記録された受信データを新規な記録媒体に複写可能な情報処理装置において、前記受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別手段と、前記記録媒体の信頼度を判定するための信頼度判定手段とを備え、前記著作権保護識別手段において著作権により保護されていると識別されたデータに対して、前記暗号化手段により暗号化を行う際に、前記信頼度判定手段において前記記録媒体の信頼度が高いと判定された場合には、前記記録媒体の固有情報に基づいて暗号鍵を生成して暗号化を行うとともに、前記信頼度判定手段において前記記録媒体の信頼度が低いと判定された場合には、当該情報処理装置の固有情報に基づいて暗号化を行うことにより、著作権を保護することを特徴とするものである。

【００１５】また、前記情報処理装置において、前記記録媒体に記録されたデータに対して用いられている暗号鍵の種類を識別するための暗号鍵識別手段を備えることが可能である。

【００１６】また、前記情報処理装置において、前記記録媒体に対してデータを暗号化して記録する際に、当該記録媒体において前記暗号鍵の種類が混在しないようにすることが可能である。

【００１７】さらに、本発明に係る情報処理装置は、データを受信するための受信手段と、該受信手段により受信した受信データが著作権により保護されたデータであるか否かを識別するための著作権保護識別手段と、前記受信データから著作権情報を検出して著作権管理情報を生成するための著作権情報管理手段と、前記受信データを暗号化するための暗号化手段と、該暗号化手段により暗号化した前記受信データを交換可能な記録媒体に記録するための記憶手段とを備え、前記記録媒体に記録された受信データを新規な記録媒体に複写可能な情報処理装

置において、当該情報処理装置の固有情報と、前記受信データの著作権情報と、前記著作権管理手段で生成した著作権管理情報とに基づいて暗号鍵を生成するための暗号鍵作成手段を備え、前記受信データに対して、前記暗号鍵作成手段で作成した暗号鍵を用いて暗号化を行い暗号化済受信データを生成し、該暗号化済受信データを前記記録媒体に記録することを特徴とするものである。

【００１８】また、前記情報処理装置において、前記受信データの著作権情報が許可した範囲において、前記暗号化済受信データと、該暗号化済受信データを復合化するための暗号鍵を送出し、新規な記録媒体に複製可能とすることができる。

【００１９】

【発明の実施の形態】以下、図面に基づいて、本発明に係る情報処理装置の一実施形態を説明する。図１は、本発明の一実施形態に係る情報処理装置の概略構成を示すブロック図である。本発明の一実施形態に係る情報処理装置１は、図１に示すように、交換可能な記録媒体２に対してデータを記録するとともに、この記録媒体２に記録されたデータを新規な記録媒体に複写することが可能な装置である。

【００２０】この情報処理装置１は、データの送受信を行うための通信機能部３と、受信したデータが著作権保護データか否かを識別するための著作権保護識別部４と、データを暗号化するためのデータ暗号部５と、データを暗号化する際に使用する暗号鍵を生成するための暗号鍵生成部６と、記録媒体２あるいは情報処理装置１の固有情報を取得して出力するための固有情報取得・出力部７と、記録媒体２の信頼度を判定するための信頼度判定部８と、記録媒体２に記録されたデータに対して使用されている暗号鍵の種類を識別するための暗号鍵識別判定部９と、記録媒体２に記録されたデータを復号化するための暗号化データ復号部１０と、復号化したデータを外部に出力するための表示・外部出力インターフェイス部１１とを備えている。また、記録媒体２には、記録されたデータに使用されている暗号鍵を認識するための暗号鍵認識手段１２が付加されている。

【００２１】この情報処理装置１において、通信機能部３で受信したデータは、著作権保護識別部４において著作権保護が行われている著作物か否かが識別される。本実施形態に係る情報処理装置１では、データの種類（ＤＶＤあるいはＤＶＣ等）毎に定められている規格に基づいて、著作権保護の識別を行なう。なお、本実施形態に係る情報処理装置１では、著作権保護が行われていない著作物の暗号化（鍵）については特定しないことを前提としているため、著作権保護が行われているデータの暗号化のみについて説明する。

【００２２】次に、図２に示すフローチャートに基づいて、本実施形態に係る情報処理装置１の動作を説明する。本実施形態に係る情報処理装置１では、通信機能部３により、通信網を介してデータを受信し、著作権保護識別部４により、著作権保護が行われているデータか否かを識別する。そして、著作権保護が行われているデータである場合には、図２に示すように、暗号鍵識別判定部９により、交換可能な記録媒体２に記録されている暗号鍵の有無を判断する（Ｓ０ａ）。

【００２３】ここで、暗号鍵が無い場合には、信頼度判定部８により、記録媒体２から読み出した信頼度に関するデータを収集して信頼度の判定（Ｓ０ｂ）を行う。一方、暗号鍵がある場合には、当該暗号鍵が記録媒体２の固有情報か否かを判別し（Ｓ１）、記録媒体２の固有情報である場合には、信頼度判定部８により、記録媒体２から読み出した信頼度に関するデータを収集して信頼度の判定（Ｓ０ｂ）を行う。

【００２４】信頼度に関するデータは、記録媒体２の種類により異なるが、例えば、記録媒体２にアクセスされた回数を初期情報エリアに書き込んでおく。そして、アクセス累積回数情報を読み出し、予め情報処理装置１のＲＯＭ等に設定されたアクセス回数の規定値と比較することにより信頼度を判定する。また、例えば、所定のタイミングで、記録媒体２の特定の空きエリアに信頼度測定用信号を記録するとともに、この信頼度測定用信号を再生し、再生時のエラー値と予め情報処理装置１のＲＯＭに設定されたエラー値とを比較することにより信頼度を判定する方法がある。記録媒体２としてＥＥＰＲＯＭを使用した場合には、およその書き換え寿命は数十万回程度と言われている。

【００２５】信頼度の判定処理（Ｓ０ｂ）において記録媒体２の信頼度が設定値以上（信頼度が高い）であると判定された場合には、固有情報取得・出力部７により、記録媒体２の固有情報を取得する（Ｓ２）。また、記録媒体２の信頼度が設定値以下（信頼度が低い）であると判定された場合、および暗号鍵の判別処理（Ｓ１）において記録媒体２の固有情報でないと判別された場合には、固有情報取得・出力部７により、情報処理装置１の固有情報を取得する（Ｓ３）。

【００２６】記録媒体２の固有情報とは、記録媒体２毎に異なる情報（例えば製造番号等の連続する番号など）のことをであり、情報処理装置１の固有情報とは、情報処理装置１毎に異なる情報（例えばＲＯＭ格納された製造番号やＣＰＵ毎に割り振られた識別番号など）のことである。また、記録媒体２の固有情報は、予め記録媒体２の初期情報として格納されているものとし、情報処理装置１の固有情報は、予め情報処理装置１内のＲＯＭに格納されているものとする。

【００２７】暗号鍵生成部６では、固有情報取得・出力部７で取得した各固有情報に基づいてそれぞれ暗号鍵を生成する（Ｓ４，Ｓ５）。続いて、データ暗号化部５により、暗号鍵生成部６で生成した暗号鍵に基づいて、受

信したデータを暗号化する（Ｓ６）。暗号化されたデータは、記録媒体２に記録保存されると同時に、暗号鍵認識手段１２により、記録媒体２の固有情報に基づいて生成した暗号鍵か（Ｓ７）、情報処理装置１の固有情報に基づいて生成した暗号鍵か（Ｓ８）が判別される。

【００２８】暗号鍵認識手段１２による暗号鍵の認識方法は、前記何れかの暗号鍵を、データとして記録媒体２に関連付けして記録する方法を用いることができる。また、前記何れかの暗号鍵を印刷したり、凹凸でマーキングすることにより、記録媒体２に物理的に認識ができる方法を用いることもできる。

【００２９】また、既に当該情報処理装置１を用いてデータが記録されている記録媒体２が、情報処理装置１に装着された場合には、記録媒体２の暗号鍵認識手段１２において暗号鍵を判別することができるので、ステップ１（Ｓ１）で判別した暗号鍵が情報処理装置１の固有情報に基づいて生成した暗号鍵であれば、情報処理装置１の固有情報に基づいて生成した暗号鍵により受信データの暗号化を行う。このように、暗号鍵認識手段１２による判別（Ｓ１）を、記録媒体２の信頼性の判定（Ｓ０ｂ）よりも優先させることにより、記録媒体２に対する暗号鍵方式の混在を防止することができる。

【００３０】また、ステップ１（Ｓ１）で判別した暗号鍵が記録媒体２の固有情報に基づいて生成した暗号鍵であった場合には、記録媒体２の信頼度判定（Ｓ０ｂ）を行なう。そして、信頼度が低いと判定された場合には、記録媒体２を交換して、新規な記録媒体２によりデータの記録を行うように警告を発する。ここで、ユーザが記録媒体２の交換を拒否（信頼性が低いままの記録媒体２でデータを追加する）した場合には、記録媒体２の固有情報に基づいて生成した暗号鍵によりデータの暗号化を行なう。

【００３１】また、記録媒体２の信頼度判定処理（Ｓ０ｂ）において、情報処理装置１の固有情報に基づいて暗号鍵を生成する場合の回数の上限値は、前記受信データの著作権保護データ内における複写回数の指定により制限してもよい。

【００３２】記録媒体２に保存された暗号化データは、記録媒体２の暗号鍵認識手段１２により認識され、暗号鍵識別判定部９により暗号鍵の種類が判定されて暗号鍵が得られる。そして、暗号化データ復号部１０により、暗号鍵と記録媒体２に記録されている暗号化データに基づいてデータが復号される。復号されたデータは、表示・外部出力インターフェイス部１１に入力され、夫々の用途に使用することができる。

【００３３】次に、本発明に係る情報処理装置の他の実施形態を説明する。

【００３４】図３は、本発明の他の実施形態に係る情報処理装置の概略構成を示すブロック図である。本発明の他の実施形態に係る情報処理装置２１は、図３に示すように、データの送受信を行なうための通信機能部２３と、受信したデータが著作権保護データか否かを識別するための著作権保護識別部２４と、データを暗号化するためのデータ暗号部２５と、データを暗号化する際に使用する暗号鍵を生成するための暗号鍵Ａ生成部２６および暗号鍵Ｂ生成部２７と、情報処理装置２１の固有情報を取得して出力するための固有情報取得・出力部２８と、受信データから取得される著作権情報を管理するための著作権情報管理部２９と、記録媒体２２に記録されたデータを復号化するための暗号化データ復号部３０と、復号化したデータを外部に出力するための表示・外部出力インターフェイス部３１とを備えている。また、記録媒体２２には、記録されたデータに使用されている暗号鍵情報を管理するための鍵情報管理部３２が付加されている。情報処理装置２１の固有情報とは、情報処理装置２１毎に異なる情報、例えばＲＯＭ内部に格納されている製造番号などのことである。

【００３５】この情報処理装置２１において、通信機能部２３で受信したデータは、著作権保護識別部２４において著作権保護の対象データか否かが識別される。本実施形態に係る情報処理装置２１では、データの種類（ＤＶＤやＤＶＣ等）毎に定められている規格に基づいて、著作権保護の識別を行なう。

【００３６】次に、図４に示すフローチャートに基づいて、本実施形態に係る情報処理装置２１の動作を説明する。本実施形態に係る情報処理装置２１では、通信機能部２３により、通信網を介してデータを受信し、著作権保護識別部２４により、著作権保護の対象データか否かを識別する。そして、著作権保護のデータである場合には、図４に示すように、著作権者からデータの複製が許可されているか否かの情報を取得して当該制限内容を判断する（Ｓ１１）。

【００３７】ここで、データの複製が許可されていない場合には、複製許可回数と複製許可回数残回数をともにゼロとして（Ｓ１２）、複製を禁止する（Ｓ１２）。そして、複製許可回数を取得するとともに（Ｓ１３）、複製許可残回数を取得し（Ｓ１４）、取得した複製許可回数および複製許可残回数に基づいて、暗号鍵Ａ生成部２６により暗号鍵Ａを生成する（Ｓ１５）。したがって、暗号鍵Ａには、著作権情報に基づく複製制限情報が含まれることとなる。

【００３８】また、固有情報取得・出力部２８から装置固有情報を取得し（Ｓ１６）、この装置固有情報および複製許可回数に基づいて、暗号鍵Ｂ生成部２７により暗号鍵Ｂを生成する（Ｓ１７）。したがって、暗号鍵Ｂには、装置固有情報と複製可否情報が含まれることとなる。続いて、データ暗号部２５において、生成された暗号鍵Ａと暗号鍵Ｂとに基づいて、受信したデータを暗号化する（Ｓ１８）。暗号化されたデータは、記録媒体２２に保存され（Ｓ１９）、暗号化に使用した暗号鍵Ａと

暗号鍵Ｂの情報は、鍵情報管理部３２で管理される。

【００３９】記録媒体２２に記録された暗号化データは、鍵情報管理部３２で管理される情報に基づいて、暗号化データ復号部３０により、各暗号鍵と記録媒体２２に記録されている暗号化データから復号され、表示・外部出力インターフェイス部３１へ送られ、表示あるいは出力される。

【００４０】

【発明の効果】本発明に係る情報処理装置によれば、著作権により保護されたデータが記録されている記録媒体の信頼度判定を行い、記録媒体の信頼度が高い場合には記録媒体の固有情報に基づいて暗号鍵を生成し、記録媒体の信頼度が低くなると情報処理装置の固有情報に基づいて暗号鍵が生成される。したがって、記録媒体の信頼度が低くなった場合には、新規な記録媒体と入れ替えて複写を行うことが可能になり、重要なデータを失うおそれがなくなる。

【００４１】また、新規な記録媒体に複写された複写データから暗号鍵を生成する場合には、この新規な記録媒体の信頼性判定を行う（当然信頼性が高い）ので、当該新規な記録媒体の固有情報に基づいて暗号鍵が生成され、著作権が保護される。

【００４２】また、本発明に係る情報処理装置によれば、記録媒体に対して記録されたデータの暗号鍵方式を識別することができるので、使用者が暗号鍵の種類を判断して情報処理装置に入力する必要はなく、情報処理装置において自動的に暗号鍵の種類が認識される。

【００４３】また、本発明に係る情報処理装置によれば、記録媒体に記録されたデータに対して暗号鍵の種類が混在することがないので、データの管理が容易となる。

【００４４】また、本発明に係る情報処理装置によれば、情報処理装置の固有情報と、受信データの著作権情報と、著作権情報管理手段で生成した著作権管理情報とに基づいて暗号鍵が生成される。したがって、暗号鍵を生成するため著作権保護の対象となる暗号化データを複製しようとした場合に、暗号鍵が保持する複製制限情報および複製可否情報に基づいた複製管理が可能となる。さらに、暗号鍵は装置固有情報を保持しているので、ユーザーが他の情報処理装置へのデータ移動を望む場合であっても、著作権保持者がその行為を許可しているのであれば、装置固有情報を参照しない状態における一過性の複製が可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る情報処理装置の概略構成を示すブロック図である。

【図２】本発明の一実施形態に係る情報処理装置の動作を示すフローチャートである。

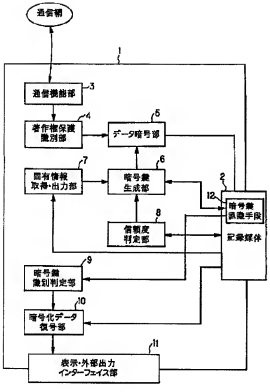
【図３】本発明の他の実施形態に係る情報処理装置の概略構成を示すブロック図である。

【図４】本発明の他の実施形態に係る情報処理装置の動作を示すフローチャートである。

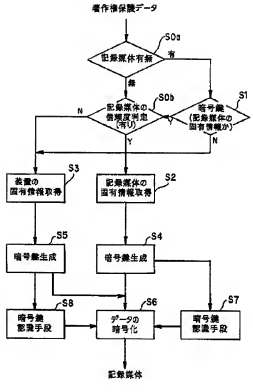
【符号の説明】

１、２１　情報処理装置
２、２２　記録媒体
３、２３　通信機能部
４、２４　著作権保護識別部
５、２５　データ暗号部
６　暗号鍵生成部
７　固有情報取得・出力部
８　信頼度判定部
９　暗号鍵識別判定部
１０、３０　暗号化データ復号部
１１、３１　表示・外部出力インターフェイス部
１２　暗号鍵認識手段
２６　暗号鍵Ａ生成部
２７　暗号鍵Ｂ生成部
２８　固有情報取得・出力部
２９　著作権情報管理部
３２　鍵情報管理部

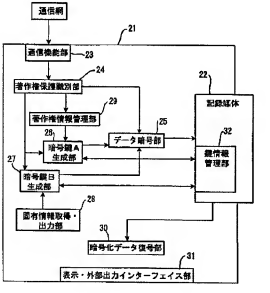
【図１】


通信網
1
通信機能部
3
著作権保護識別部
4
データ暗号部
5
固有情報取得・出力部
7
暗号鍵生成部
6
2
12
暗号鍵識別手段
信頼度判定部
8
記録媒体
暗号鍵識別判定部
9
暗号化データ復号部
10
表示・外部出力インターフェイス部
11

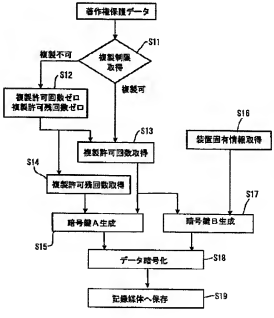
【図２】


著作権保護データ
S0a
記録媒体有無
有
無
S0b
記録媒体の信頼度判定（有り）
N
Y
S1
暗号鍵（記録媒体の固有情報か）
N
Y
S3
装置の固有情報取得
S2
記録媒体の固有情報取得
S5
暗号鍵生成
S4
暗号鍵生成
S8
暗号鍵識別手段
S6
データの暗号化
S7
暗号鍵識別手段
記録媒体

【図３】


通信網
21
通信機能部
23
著作権保護識別部
24
22
記録媒体
著作権情報管理部
29
データ暗号部
25
25
暗号鍵Ａ生成部
32
鍵情報管理部
27
暗号鍵Ｂ生成部
固有情報取得・出力部
28
30
暗号化データ復号部
表示・外部出力インターフェイス部
31

【図４】


著作権保護データ
S11
複製制限取得
複製不可
複製可
S12
複製許可回数ゼロ
複製許可残回数ゼロ
S13
複製許可回数取得
S14
複製許可残回数取得
S15
暗号鍵Ａ生成
S16
装置固有情報取得
S17
暗号鍵Ｂ生成
データ暗号化
S18
記録媒体へ保存
S19